

Southeastern University

Protects Student Data and Privacy,
While Building the Foundation for
Secure AI Adoption

Case Study | Customer Story

Overview

Southeastern University (SEU) is a faith-based higher education institution based in Lakeland, Florida. The university manages sensitive information spanning students, applicants, faculty, staff, financial operations, and academic records across a diverse technology environment.

As SEU strengthened its cybersecurity program, its cybersecurity team wanted to move beyond fragmented visibility and better understand where sensitive information was located, whose data it was, who could access it, and how it should be protected. With Lightbeam, SEU has established a foundation for data security across its cloud and on-premises environment. The university is using that foundation to reduce sensitive data risk, strengthen access and retention controls, improve regulatory compliance, and ultimately enable the responsible use of AI.



“If I had to describe the value that Lightbeam has given SEU, I would say in one word: visibility. When it comes to data security, that’s foundational.”

Joshua Rhoden • Executive Director of IT Operations & Security, Southeastern University

Customer Story Summary

Challenges	Approach	Results
• Sensitive data spread across cloud, SaaS, collaboration, and on-premises systems • Limited consolidated visibility into where sensitive data was stored and who could access it • Oversharing and open-access links • Different requirements for FERPA, GLBA, PCI, PII, financial, and other regulated information • Lean cybersecurity team without resources to manually discover and govern data • Growing AI adoption creating new data-control requirements	• Connected Lightbeam to Google, Microsoft, databases, file servers, and other data sources • Discovered and classified sensitive information across 180+ TB of data • Created data identities for students, staff, faculty, applicants, and other entities • Developed SEU-specific classifications for academic records, student financial information, loans, tuition, FAFSA, and other regulated data • Identified open access and excessive sharing • Established a foundation for retention, access governance, and AI data security	• Visibility across 180+ TB of data and 7.6 million files • 642,000 files containing sensitive information identified • Approximately 1.7 million entities created • Continuous monitoring across 13 data sources • Greater context and accuracy by understanding whose sensitive data is contained in files • Foundation for least-privilege access, retention, compliance, and responsible AI adoption

Challenge

Moving Beyond “Shooting in the Dark”

Southeastern University’s cybersecurity team knew sensitive information existed throughout a complex environment that included multiple collaboration platforms, SaaS applications, cloud environments, databases, and on-premises systems.

What the team lacked was a consolidated view of exactly where that information lived, what it contained, whose data it was, and who could access it.

SEU initially relied on functionality built into platforms such as Google Workspace and Microsoft Office365 to locate sensitive data. But managing discovery separately within each system could not provide the university with the consistent, cross-platform inventory or the ability to take action to reduce risk.

The university is responsible for protecting student records and financial information governed by regulations including FERPA and GLBA, along with PCI data, personally identifiable information (PII), and other regulated information.

For SEU, meeting those requirements is more than a compliance exercise. The university views data security and privacy as part of the trust students and their families place in the institution.

The team also began identifying risky sharing behavior. Files containing sensitive information could be publicly accessible to anyone with a link or shared with groups much larger than the population that legitimately needed access.

For a lean cybersecurity organization, attempting to identify and manage those risks manually across Google Workspace, Microsoft 365, cloud platforms, and on-premises systems was not sustainable.

Solution

Building an Unified View of University Data and Cybersecurity Risk

SEU deployed Lightbeam across its cloud and on-premises environment to create a unified map of sensitive information using the Lightbeam Data Identity Graph technology.

The university connected Lightbeam to Google and Microsoft environments, file servers, databases, email, and other data sources. Lightbeam now provides continuously updated visibility across more than 180 TB of data, 7.6 million files, and 13 monitored data sources.

Lightbeam has identified approximately 642,000 files containing sensitive data and more than 32 million sensitive-data attributes, providing SEU with a foundation for understanding its data landscape at a scale that would have been impractical to manage manually.

But discovery alone was only the first step.

Understanding Whose Data It Is

For Southeastern University, sensitive information does not all carry the same meaning or require the same treatment.

Student information, faculty and employee information, applicant information, business financial records, student financial aid information, payment-card information, and institutional data can each carry different regulatory requirements and security policies. Using the Lightbeam Data Identity Graph, SEU can associate sensitive information with the individual or entity it belongs to.

The university has established approximately 1.7 million entities, creating data identities across students, staff, faculty, applicants, and institutional populations.

That identity context lets SEU move beyond simply knowing that a document contains sensitive information.

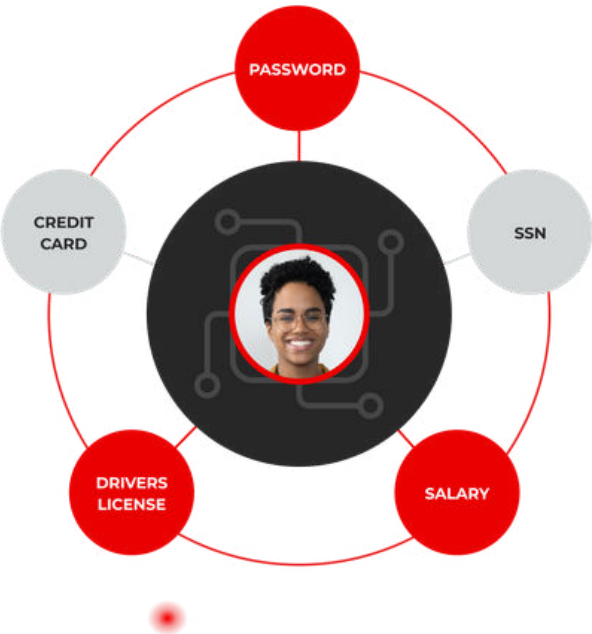
For example, the university must distinguish between student financial information and financial information associated with university business operations.

The protections, retention requirements, and policies applied to those categories may be very different.

SEU used Lightbeam to develop custom granular classifications for academic records, student financial information, loans, tuition, FAFSA information, and other university-specific data.

Those classifications provide the context necessary to begin applying the appropriate retention, access, and compliance policies to different categories of data.

Identity can also improve incident response. If sensitive information is compromised, SEU can determine which people are actually affected rather than assuming an entire population may have been exposed.



“The entity feature is pretty important because then we can identify personnel as well as students and applicants, the data that we’ve gathered on them, and what sensitive data belongs to each entity.”

Heather De La Cruz • Assistant Director of Cybersecurity, Southeastern University

Results

Turning Visibility Into Risk Reduction

With a dependable inventory of sensitive data in place, Southeastern University is moving from discovery toward automated actions that reduce risk. One immediate area of value has been finding information that was more broadly accessible than its owners realized. Lightbeam has helped SEU identify open-access links and other exposure in cloud environments so that the security team can remediate unnecessary access and apply a least privilege approach to access reviews. The platform currently maps permissions across SEU's environment and identifies users and groups with access to sensitive information. Baseline governance policies are in place to detect external exposure, open access, and data-minimization risks.

SEU plans to work with data owners to reduce unnecessary access. Information that may currently be available to an entire group, for example, can be restricted to the small number of people who actually require it. Retention represents another important opportunity. SEU can identify information subject to retention requirements such as student loan or FAFSA records, while also locating sensitive information the university no longer has a legitimate reason to retain. Minimizing redundant, obsolete, and trivial data that contains sensitive data has the benefit of reducing risk, eliminating legal liability, and reducing storage costs.

The university is now progressing toward automated, label-based retention and access enforcement while continuing to refine classifications and policies with university data owners. For SEU's lean security organization, automation and context are particularly important. That context helps SEU move beyond basic discovery toward more precise decisions about access, retention, compliance, and risk.



"Lightbeam isn't only looking for keywords and patterns. It's actually able to see inside your data and get context on it. What we've found is that it's able to have a lot more true positives when it finds sensitive data."

Joshua Rhoden • Executive Director of IT Operations & Security, Southeastern University

Preparing to Safely Enable AI

Southeastern University does not view AI solely as a security risk. The university actively encourages appropriate AI use by students, faculty, and staff.

Students can use AI for activities such as research and writing assistance, while faculty, staff, and operations teams can use AI to analyze information and automate repetitive work.

SEU sees AI as an opportunity to improve productivity and allow employees to spend more time supporting students. At the same time, widespread AI adoption introduces new questions and risks about sensitive information.

The cybersecurity team needs to understand what data is being provided to AI systems, whether providers retain that information, whether it could be used to train models, and whether an AI application should have access to the information in the first place.

SEU sees the data discovery, classification, labeling, access, and identity foundation it has established with Lightbeam as a way to address those challenges without preventing legitimate AI innovation.

The university plans to leverage Lightbeam's AI Data Security capabilities as it explores applying those to secure and enable safe AI use.

The goal is not to prohibit AI. It is to give SEU the context to determine which data can safely be used with AI and which information requires stronger AI governance and protection.



“What we want to make sure we’re able to do is protect data from AI use that could cause a security risk. If we want to restrict sensitive data, we need the ability to identify it and put policies in place that don’t allow that AI system to access it, while maybe allowing access to other information that can help automate tasks or analyze data.”

Joshua Rhoden • Executive Director of IT Operations & Security, Southeastern University

Future Plans

Southeastern University sees its current deployment as the foundation for a broader data-security, governance, and AI security program.

The university plans to continue refining its classifications and labels, finalize regulatory data retention policies, expand access governance, and implement workflows to remediate inappropriate internal and external access. As those capabilities mature, the university plans to extend that foundation to responsible AI adoption through Lightbeam's AI Data Security capabilities. For SEU, the next phase is about turning the visibility it has gained into increasingly automated controls across data access, retention, compliance, and AI.



"The value that Lightbeam has given us is immense. It's going to allow us to do so much more in protecting our students and our community."

Joshua Rhoden • Executive Director of IT Operations & Security, Southeastern University



Lightbeam

Lightbeam provides AI Guardrails for Enterprise Data, helping organizations control what sensitive data AI can reach, use, and expose. Powered by the patented Lightbeam Data Identity Graph, Lightbeam maps sensitive data to identity, access, business context, policy, and risk so teams can stop shadow AI, enforce least privilege access, reduce data exposure, automate privacy workflows, and prove controls are working. Lightbeam helps enterprises safely adopt GenAI, copilots, SaaS AI, and agents while protecting the people and businesses behind the data.

GET A DEMO

<https://lightbeam.ai>